UNITED STATES PATENT APPLICATION

Title:

THEFT PREVENTION USING LOCATION DETERMINATION

Inventors:

Animesh Mishra

Jun Shi

Harshad Junnarkar

Docket No.: 42390.P10482

Prepared by:
Richard C. Calderwood
Reg. No. 35,468

"Express mail" label no. EL034439811US

THEFT PREVENTION USING LOCATION DETERMINATION

Background of the Invention

Technical Field of the Invention

The present invention relates generally to preventing theft of devices.

Background Art

Location determination and motion detection devices are known, including such mechanisms as mercury switches, accelerometers, and global positioning system (GPS) devices. It is known to utilize such devices in a passive, queried mode to provide theft deterrence. For example, automobiles equipped with the OnStar System can be remotely disabled after the theft has been detected. However, this requires that the owner or other person notice that the automobile has been stolen. Furthermore, if the thief disables the OnStar System before the owner phones in a report of the theft, the OnStar personnel will be unable to disable the vehicle remotely.

Brief Description of the Drawings

The invention will be understood more fully from the detailed description given below and from the accompanying drawings of embodiments of the invention which, however, should not be taken to limit the invention to the specific embodiments described, but are for explanation and understanding only.

FIG. 1 illustrates one embodiment of a system which utilizes the principles of this invention, including an exemplary appliance device to be protected against theft.

FIG. 2 illustrates one embodiment of a method of operating the device to be protected against theft.

FIG. 3 illustrates another embodiment of a method of operating the device to be protected.

Detailed Description

FIG. 1 illustrates a system 10 according to this invention, including an exemplary device 12 to be protected against theft. For simplicity, the device 12 will be referred to as an appliance, but the reader will understand that it may be any type of device whatsoever, such as an automobile, a home appliance such as a refrigerator, a computer, or a television.

The appliance is coupled over a communication link to a central agency 16 service or device which may, in turn, be coupled over a notification link 18 to a law enforcement agency device 20 such as a central dispatch computer, radio, or the like. The reader will appreciate that the communication link and the notification link may utilize a telephone network, computer network, the internet, wireless, cellular, satellite, laser, audio, or any other suitable mechanism.

The appliance includes a local policy enforcer 30, a location determiner 32 which may be a location determination device or a motion detection device, a user authenticator 34, an appliance disabler/enabler, a functional unit 38, and a communication interface 39.

The local policy enforcer may constitute a software-programmed microprocessor, hard-wired logic, or other suitable means of performing the functionality of the local policy enforcer, which will be described below.

The location determiner may be as simplistic as a mercury switch, which detects only motion but not relative position much less absolute position; or it may be a more complex device such as a GPS receiver, which detects absolute position as well as motion; or it may be something in between such as an accelerometer, which detects motion and relative position but not absolute position.

The user authenticator may be as simple as a key device which may readily be possessed by any user; or it may be as complex as a biometric identity analyzer which is specific to a single individual user; or it may be something in between such as a password system. It may include simply a data gathering mechanism, but it may also include means for applying policies or comparing the data against, for example, a locally-stored copy of known-valid data, such as from a previously sampled user input.

The enabler/disabler is adapted for enabling and/or disabling the functional unit. In some embodiments, the functional unit may be in a default state of disablement until the enabler/disabler enables it. In other embodiments, the functional unit may be enabled unless the enabler/disabler disables it.

The functional unit provides the functionality of the appliance and would typically be found in an appliance which lacks the features of this invention; for example, in the case of a television, the functional unit might be the tuner or the display or the on/off switch.

The appliance's communication interface is suitably adapted for communicating over the chosen communication link. In one embodiment, the location determiner and user authenticator may be coupled to the local policy enforcer, and the local policy enforcer may be coupled to the

communication interface. Other configurations will, of course, be apparent given the teachings of this patent.

The central agency service or device 16 includes a communication interface 44 which is suitably adapted for communicating with the appliance over the communication link. It further includes a remote policy enforcer 40, an appliance registry 42, an optional user authenticator 43, and an optional notification interface 46. The remote policy enforcer may constitute a software-programmed microprocessor, hard-wired logic, or other suitable means of performing the functionality of the remote policy enforcer, which will be described below. The appliance registry may include a database or other suitable data storage and retrieval system, and a storage device for housing the database, such as a hard disk, a tape drive, a DVD-R drive, semiconductor memory, or other suitable storage means. The user authenticator 43 will not typically include a user data input gathering device, such as the biometric apparatus or password input means of the user authenticator 34 of the appliance. The central agency's user authenticator 43 may gather data through such user data input gathering device, and apply locally-held knowledge or policies, such as by comparing the user's biometric information against a stored database (not shown). The notification interface is suitably adapted for communicating over the chosen notification link.

FIG. 2 shows a flowchart which illustrates one exemplary embodiment of a method of operating the appliance of FIG. 1, to which the reader is also referred. FIG. 2 should also be understood to represent one or more information storage devices having stored thereon instructions, operations, routines, control codes, or the like, which, when loaded into or executed upon a programmed computer device, a programmable logic device, or the like, will cause such device to execute the exemplary method.

The method begins (59) with the appliance being disabled (60). The appliance determines (61), via its location determiner, where the appliance is presently located. In the simplistic case of e.g. a mercury switch, what is determined is simply that the appliance has moved, rather than an absolute or relative position.

Then, the local policy enforcer checks (62) whether that location meets guidelines of a local policy. A variety of local policies may be utilized in practicing this invention. Examples, given by way of illustration and not exhaustive enumeration, include:

- no motion

- motion over short enough distance that the appliance is likely to still be within the user's house
- previously approved location

If the location meets the local policy, then the local policy enforcer enables (63) the appliance. In various embodiments, this may constitute providing power to the functional unit. In other embodiments, it may constitute unlocking the functional unit. The reader will appreciate that a suitable dis/enablement mechanism may readily be chosen for a given appliance, given the teachings of this patent. The reader will also appreciate that various mechanisms may be adapted to disable the appliance, to enable the appliance, or to do both; thus the term "dis/enablement". Once the appliance is enabled, the method may end (64) until a next time that, for example, it is powered on, or a next time that it is moved.

If the location does not meet the local policy, then the appliance will communicate information over the communication interface and communication link to the central agency. In various embodiments, the information sent to the central agency may be, for example, the location of the appliance, the fact that the appliance has moved, an indication of in what manner the local policy was failed, a unique identification of the appliance, an identification of the owner (authorized user) of the appliance, a most recent location which did not fail the local policy, or any combination of such information or other suitable information.

The central agency's remote policy enforcer will make a determination (65) of whether the new location (or other submitted data) meets a remote policy. A variety of remote policies may be utilized in practicing this invention, such as, for example:

- motion over a short enough distance that theft is unlikely
- motion to a pre-approved location such as a repair facility
- motion to a new location authorized by the owner pursuant to a sale of the appliance
- Nth instance of motion where N is less than a predetermined value
- total motion during the lifetime of the appliance is less than a predetermined maximum, such as a prepaid rental mileage
- motion to a location still within a country within which usage of the appliance is permitted by law

If the location meets the remote policy, the central agency remotely enables (66) the appliance. This may be done by sending an enablement signal or value back over the communication link, or by other suitable mechanism. In some instances, it may be desirable to have the appliance be self-enabling unless the central agency disables the appliance. Upon receipt at the communication interface of the dis/enablement signal, the local policy enforcer triggers the dis/enabler to enable or disable the functional unit.

In some embodiments, it may be desirable to update (67) the appliance registry with the new location or other information provided by the appliance or derived from such information. Once the appliance is enabled and the new information is registered, the method may end (68) until a next time it is utilized.

If the location failed the remote policy, in some embodiments the appliance may simply be disabled (not shown). In other embodiments, it may be more desirable to provide for a mechanism to allow the appliance to be used even though its movement has failed both the local and remote policies. One suitable choice is by authenticating (69) the user. This may involve the user inserting a key into the user authenticator, or the user entering a password into the user authenticator, or the user authenticator gathering biometric data about the user, such as via a thumbprint pad or an iris scan.

If the user is not authenticated, the appliance notifies (70) the central agency, which in turn may notify (71) law enforcement. In some embodiments, the authentication may be checked at the central agency rather than at the appliance; in this case, the appliance will not need to notify (70) the central agency. The central agency may provide to law enforcement any of the data which the central agency has about the user, the location and identity of the appliance, and so forth. In some embodiments, the user authenticator on the appliance may be simply a data input device (whether it be a key, a password, or a biometric input device), and the logic to determine whether the user is authentic may reside at the central agency. This would help prevent a thief from altering the output of the user authenticator, or sending back simplistic "he is authentic" types of messages. In such cases, the notification (70) to the central agency will be data to be used in a determination, rather than an outcome of a determination. The method may end (72) with the appliance being left in a disabled state, or in some embodiments, in an enabled state. In some cases, the functionality of the device (such as a defibrillator) is important enough that it is better to leave the device functioning in the hands of a possible thief. In some cases, it may be desirable to leave the device operational so that the thief is unaware that the theft has been noticed and reported to law enforcement. In some

embodiments, the law enforcement notification may be done directly by the appliance, rather than, or in addition to, by the central agency.

If the user is authenticated, the appliance is enabled (73), the register is updated (74), and the method ends (75).

In some embodiments, the local policy and/or remote policy may have dynamically adjustable guidelines. Consider the example of a golf cart. The first time the golf cart is turned on, the policies may require a user authentication. Then, as long as the golf cart does not leave the general vicinity (meaning that it is likely to still be at the same golf course), no authentication may be required. Then, when the cart suddenly moves to a different course, authentication may again be required. But then, on a second or third trip to different courses, within the same city, authentication may not be required; the policies may learn that the legitimate user has recently changed his playing habits.

FIG. 3 illustrates another embodiment of a method for practicing the invention. The method begins (80) and the appliance attempts to authenticate (81) the user. If the user is not authenticated, the appliance is disabled (82), law enforcement is notified (83), and the method ends (84). If the user is authenticated, the location of the appliance is determined (84) If the location meets the local policy (86), the appliance is enabled (87) and the new location and so forth may optionally be registered (88), then the method returns to re-checking the location, providing continuous location policy checking. If the location fails the local guidelines, then it is checked against the global guidelines (89). If it meets the local guidelines, the appliance is enabled (90) and the new location and so forth may optionally be registered (91), and the method returns to re-checking the location continuously. If the remote policy is also failed, the appliance is disabled (92), law enforcement is notified (93), and the method ends (94). Alternatively, the method could disable the appliance at the start, so it would be disabled until one of the policies enables it.

The reader will appreciate that the signals or values transmitted over the communication link and notification link may advantageously be protected by suitable means, such as by data encryption. Use of a public key system over the communication link may be used to prevent a thief from stealing the appliance and leaving a dummy device behind in place of the appliance; the public key system will enable the central agency to authenticate that the appliance is what it claims to be.

Reference in the specification to "an embodiment," "one embodiment," "some embodiments," or "other embodiments" means that a particular feature, structure, or characteristic

described in connection with the embodiments is included in at least some embodiments, but not necessarily all embodiments, of the invention. The various appearances "an embodiment," "one embodiment," or "some embodiments" are not necessarily all referring to the same embodiments.

If the specification states a component, feature, structure, or characteristic "may", "might", or "could" be included, that particular component, feature, structure, or characteristic is not required to be included. If the specification or claim refers to "a" or "an" element, that does not mean there is only one of the element. If the specification or claims refer to "an additional" element, that does not preclude there being more than one of the additional element.

The various elements of the appliance and/or central agency may be constructed in hardware, software, or a combination thereof. The phrase "device" is not necessarily limited to hardware devices, nor to discrete, stand-alone mechanisms.

Those skilled in the art having the benefit of this disclosure will appreciate that many other variations from the foregoing description and drawings may be made within the scope of the present invention. Indeed, the invention is not limited to the details described above. Rather, it is the following claims including any amendments thereto that define the scope of the invention.